HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 1.6
PHÂN TÍCH LOG HỆ THỐNG

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC 2
CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH 4
1.1 Mục đích 4
1.2 Ý nghĩa của một số lệnh dùng cho quá trình phân tích log 4
1.2.1 grep 4
1.2.1.1 Mô tả: 4
1.2.1.2 Cú pháp: 4
1.2.1.3 Ví dụ: 4
1.2.1.4 Tùy chọn hữu ích: 4
1.2.2 gawk (GNU AWK) 4
1.2.2.1 Mô tả: 4
1.2.2.2 Cú pháp: 4
1.2.2.3 Ví dụ: 4
1.2.2.4 Tính năng hữu ích: 5
1.2.3 find 5
1.2.3.1 Mô tả: 5
1.2.3.2 Cú pháp: 5
1.2.3.3 Ví dụ: 5
1.2.3.4 Ứng dụng: 5
1.2.4 secure (Tệp /var/log/secure) 5
1.2.4.1 Mô tả: 5
1.2.4.2 Cú pháp phân tích: 5
1.2.4.3 Ứng dụng: 5
1.2.5 access_log (Tệp /var/log/apache2/access.log hoặc /var/log/nginx/access.log) 6
1.2.5.1 Mô tả: 6
1.2.5.2 Cách phân tích: 6
1.2.5.3 Ứng dụng: 6
1.2.6 Tổng kết 6
CHƯƠNG 2. NỘI DUNG THỰC HÀNH 7
2.1 Chuẩn bị môi trường 7
2.2 Các bước thực hiện 7
2.2.1 Phân tích log sử dụng grep trong Linux 7
2.2.1.1 Quét cổng với Zenmap trên Kali 7

2.2.1.2 Kiểm tra nội dung website bằng curl 8
2.2.1.3 Kiểm tra file access_log trên máy nạn nhân 9
2.2.2 Phân tích log sử dụng gawk trong Linux 10
2.2.2.1 Tạo tài khoản mới trên máy Linux Internal Victim 10
2.2.2.2 Kiểm tra file log trên máy Linux Internal Victim 11
2.2.2.3 Truy vấn log từ máy Kali Attack 12
2.2.3 Phân tích log sử dụng find trong Windows 14
2.2.3.1 Sử dụng xHydra để brute-force FTP 14
2.2.3.2 Phân Tích Log FTP trên Windows Server 2019 15
KẾT LUẬN 16
TÀI LIỆU THAM KHẢO 16

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, bao gồm:

- Phân tích log sử dụng grep/gawk trong Linux
- Phân tích log sử dụng find trong Windows
- Tìm hiểu về Windows Event Viewer và auditing
- Phân tích event log trong Windows

1.2 Ý nghĩa của một số lệnh dùng cho quá trình phân tích log

Dưới đây là ý nghĩa và công dụng của một số lệnh phổ biến trong quá trình phân tích log trên hệ điều hành Linux:

1.2.1 grep

1.2.1.1 Mô tả:

Lệnh grep dùng để tìm kiếm các dòng có chứa một chuỗi hoặc một mẫu (pattern) trong tệp tin hoặc đầu ra của lệnh khác.

1.2.1.2 Cú pháp:

grep [tùy chọn] "chuỗi_cần_tìm" tệp_log

1.2.1.3 Ví dụ:

Tìm các dòng có chứa từ “error” trong tệp syslog:

grep "error" /var/log/syslog

1.2.1.4 Tùy chọn hữu ích:

- -i: Không phân biệt chữ hoa/chữ thường
- -r: Tìm kiếm đệ quy trong thư mục
- -n: Hiển thị số dòng

1.2.2 gawk (GNU AWK)

1.2.2.1 Mô tả:

gawk là phiên bản mở rộng của awk, dùng để xử lý và phân tích dữ liệu dạng văn bản theo cột.

1.2.2.2 Cú pháp:

gawk '{câu_lệnh_xử_lý}' tệp_log

1.2.2.3 Ví dụ:

Lấy cột thứ 1 và 4 trong tệp log access.log:

gawk '{print $1, $4}' /var/log/apache2/access.log

1.2.2.4 Tính năng hữu ích:

- Chia nhỏ log thành các cột để xử lý dễ dàng hơn
- Có thể kết hợp với grep, sort, uniq để phân tích sâu hơn

1.2.3 find

1.2.3.1 Mô tả:

Dùng để tìm kiếm tệp tin trong hệ thống theo tên, thời gian chỉnh sửa, kích thước, v.v.

1.2.3.2 Cú pháp:

find [thư_mục] [tùy_chọn] [điều_kiện]

1.2.3.3 Ví dụ:

- Tìm tất cả các tệp log trong /var/log:

  find /var/log -name ".log"*

- Tìm các tệp log được chỉnh sửa trong 7 ngày qua:

  find /var/log -name ".log" -mtime -7*

1.2.3.4 Ứng dụng:

- Tìm kiếm nhanh các tệp log để phân tích
- Xóa các tệp log cũ để tiết kiệm dung lượng

1.2.4 secure (Tệp /var/log/secure)

1.2.4.1 Mô tả:

Đây là tệp log chứa thông tin về xác thực, đăng nhập, SSH, và quyền root trên hệ thống Linux.

1.2.4.2 Cú pháp phân tích:

- Kiểm tra đăng nhập thất bại:

  grep "Failed password" /var/log/secure

- Xem các lần đăng nhập SSH thành công:

  grep "Accepted password" /var/log/secure

1.2.4.3 Ứng dụng:

- Theo dõi bảo mật hệ thống
- Phát hiện các cuộc tấn công brute-force

1.2.5 access_log (Tệp /var/log/apache2/access.log hoặc /var/log/nginx/access.log)

1.2.5.1 Mô tả:

Đây là tệp log ghi lại tất cả các yêu cầu HTTP đến máy chủ web Apache/Nginx.

1.2.5.2 Cách phân tích:

- Xem 10 yêu cầu gần nhất:

  tail -n 10 /var/log/apache2/access.log

- Đếm số lượt truy cập từ một IP cụ thể:

  grep "192.168.1.100" /var/log/apache2/access.log | wc -l

- Lấy danh sách các IP truy cập nhiều nhất:

  awk '{print $1}' /var/log/apache2/access.log | sort | uniq -c | sort -nr | head

1.2.5.3 Ứng dụng:

- Theo dõi lượng truy cập vào website
- Phát hiện các cuộc tấn công DDoS

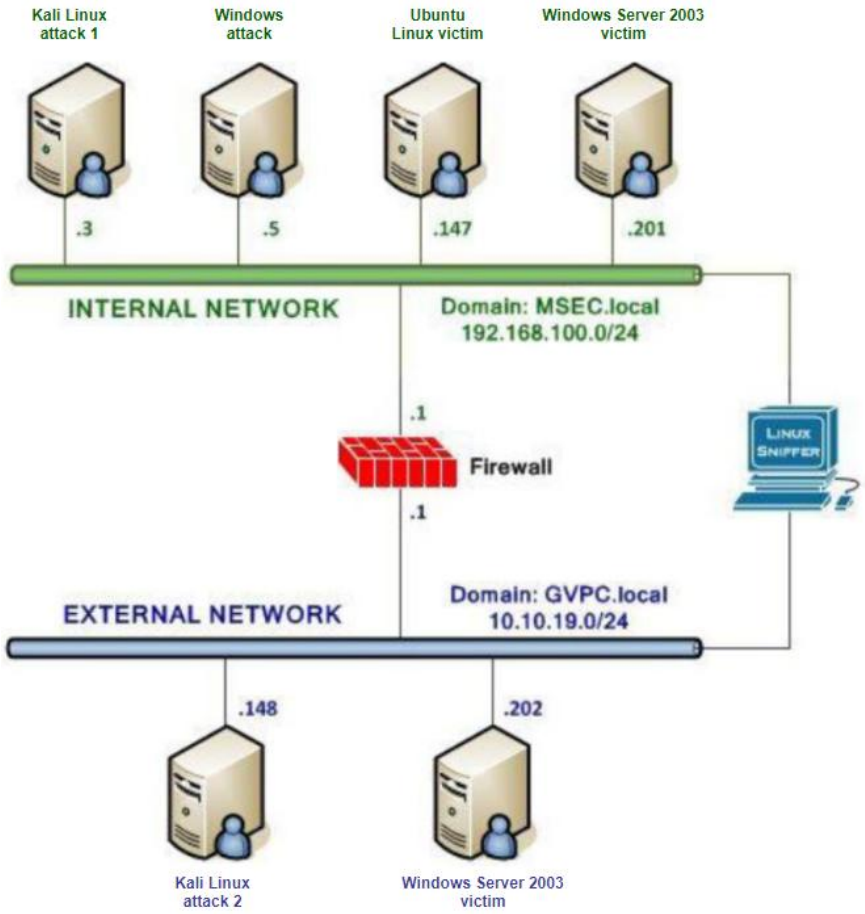
1.2.6 Tổng kết

Lệnh	Công dụng chính
grep	Tìm kiếm trong log
gawk	Xử lý và phân tích dữ liệu theo cột
find	Tìm kiếm tệp log theo điều kiện
secure	Log về xác thực và SSH
access_log	Log về truy cập web

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation (hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5.

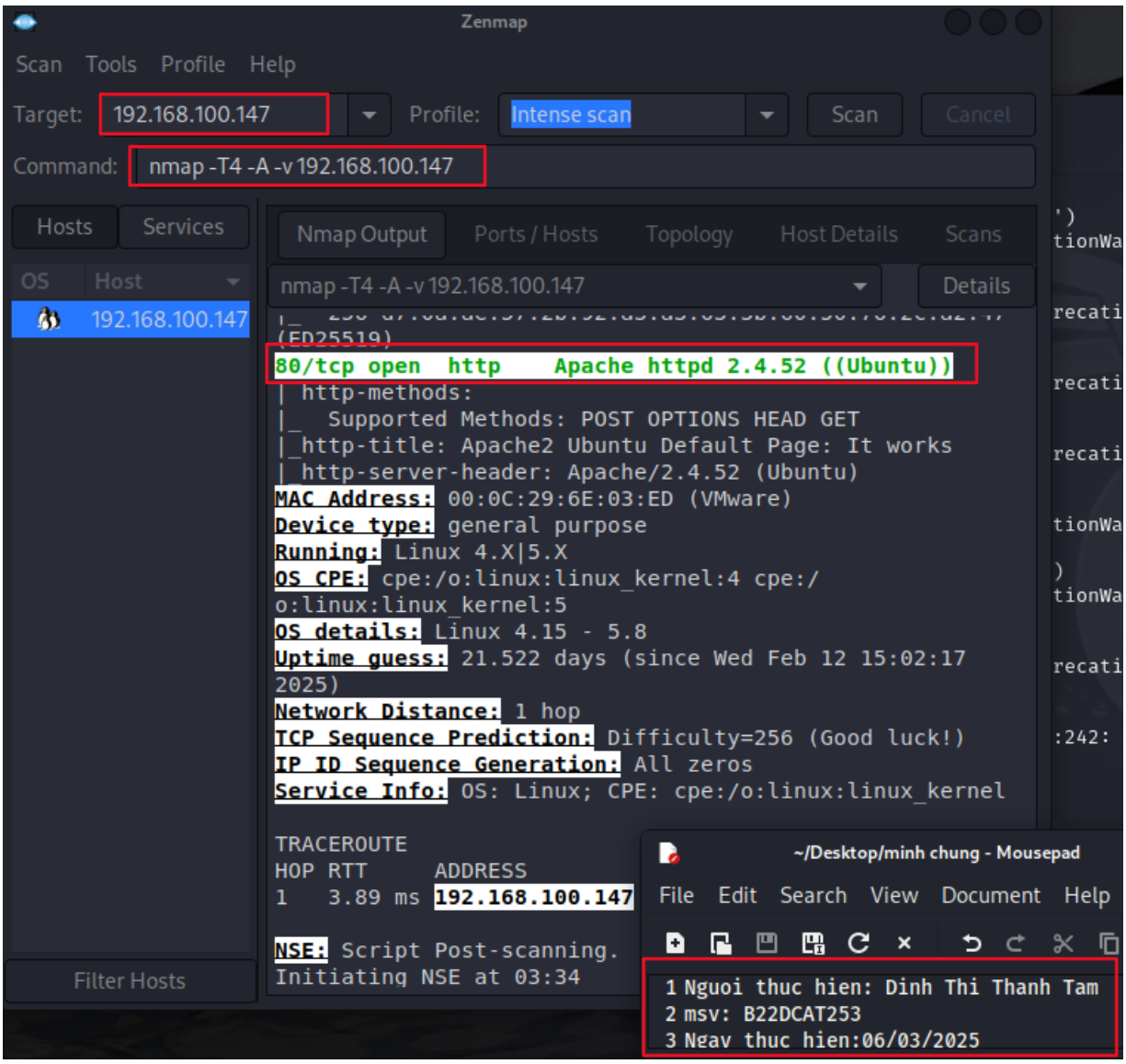


2.2 Các bước thực hiện

2.2.1 Phân tích log sử dụng grep trong Linux

2.2.1.1 Quét cổng với Zenmap trên Kali

- Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ *192.168.100.147* (Máy Linux victim)
    - Nhập vào ô Target: 192.168.100.147
    - Nhập vào ô Command: nmap -T4 -A -v 192.168.100.147
    - Nhấn Scan để bắt đầu quét.
    - Nếu thấy cổng 80/tcp mở với Apache/2.4.52, tiếp tục bước tiếp theo.

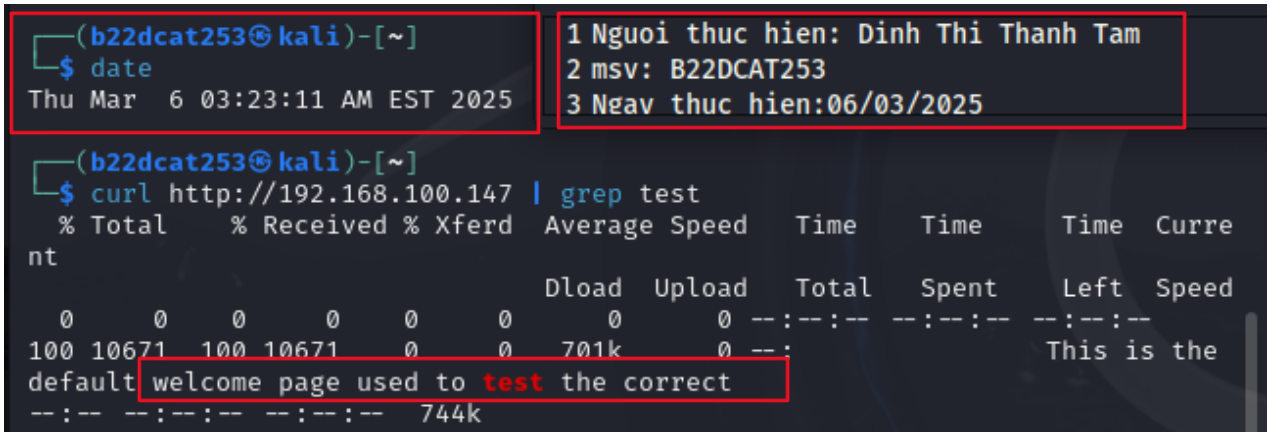


2.2.1.2 Kiểm tra nội dung website bằng curl

- Mở terminal trên Kali và chạy:

  curl http://192.168.100.147 | grep test

  ➔ Nếu có từ khóa "test", tiếp tục bước tiếp theo.



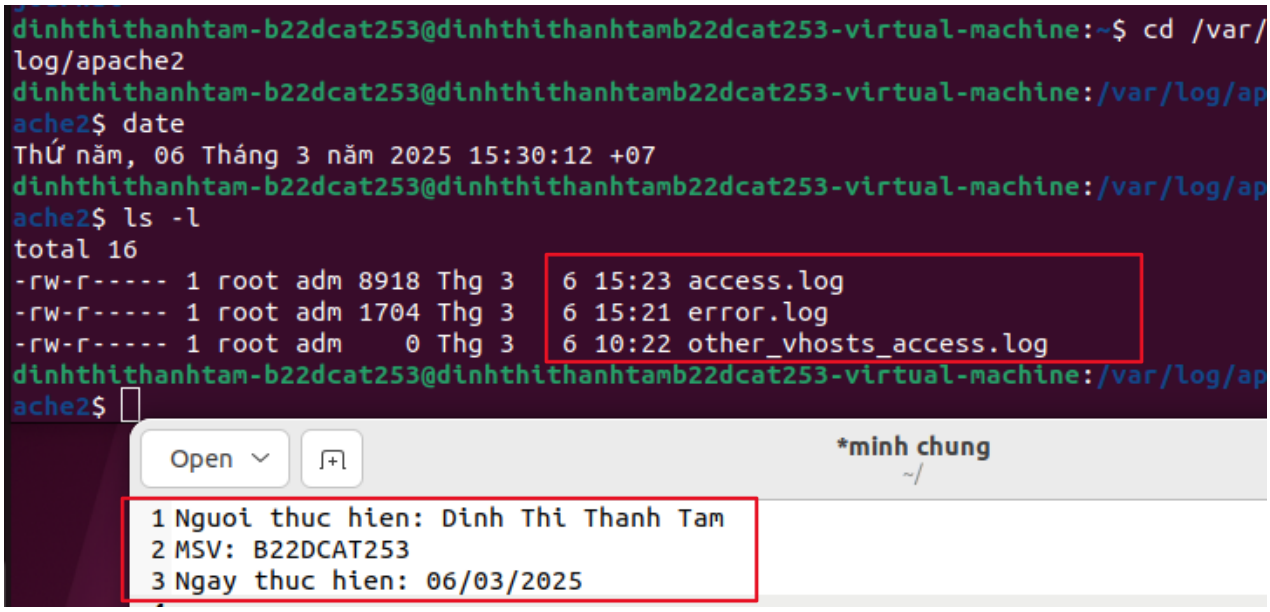
2.2.1.3 Kiểm tra file access_log trên máy nạn nhân

- Trên máy Linux nạn nhân, mở terminal và di chuyển đến thư mục chứa log của Apache:

  cd /var/log/apache2

- Liệt kê các file log:

  ls -l



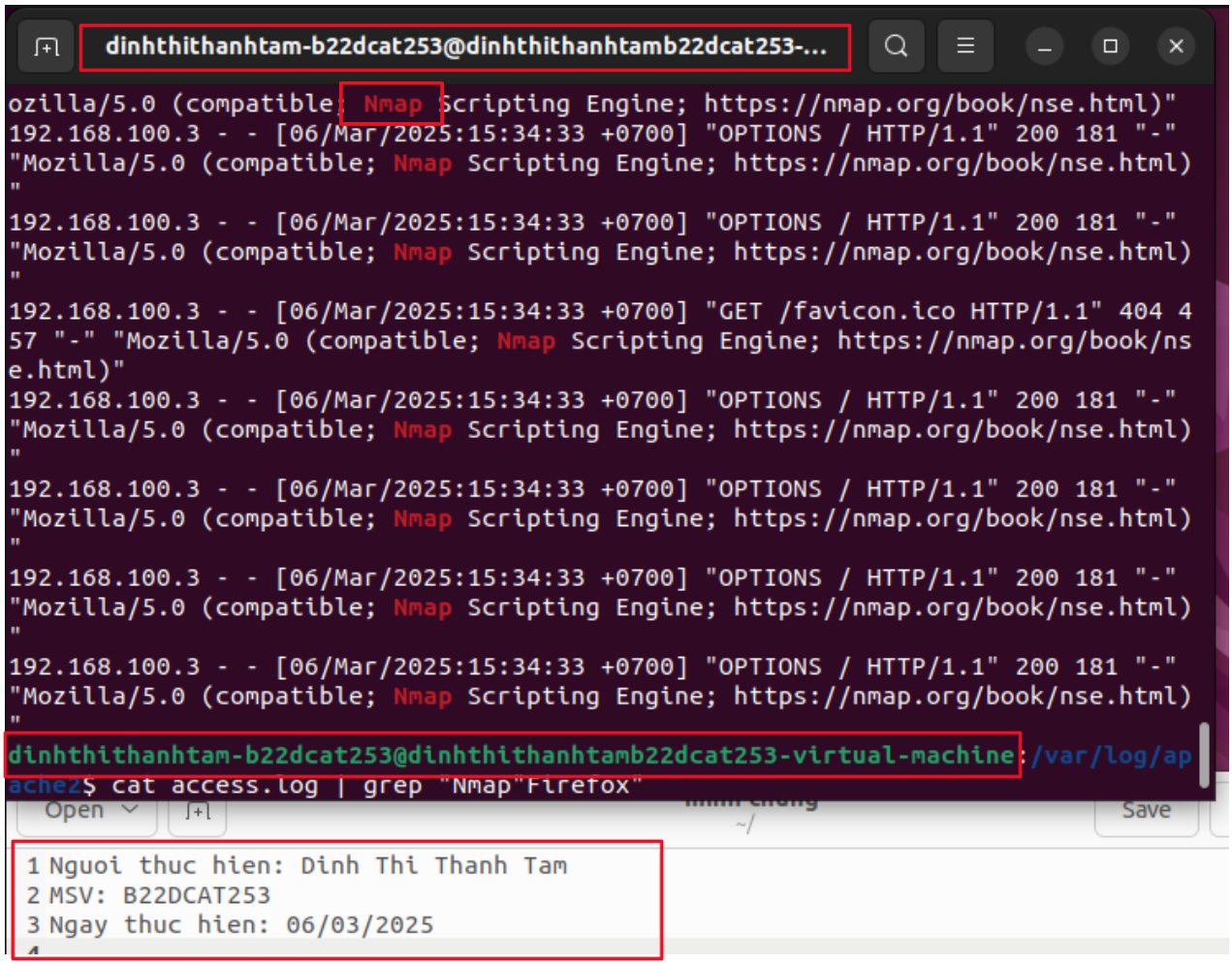
- Mở file access_log để kiểm tra các request:

  cat access.log | grep "curl"

- Dòng log này cho thấy có một request từ IP 192.168.100.3 truy cập vào server Apache bằng lệnh curl. Cụ thể:
  - Thời gian: 06/Mar/2025 15:23:42
  - Phương thức HTTP: GET / HTTP/1.1
  - Mã phản hồi: 200 (thành công)

  - Kích thước response: 10926 bytes
  - User-Agent: "curl/8.11.0" (tức là request được gửi từ curl phiên bản 8.11.0)

- Khi đã mở được file access_log trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm ví dụ: Nmap, Firefox, curl, …



```
ozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "GET /favicon.ico HTTP/1.1" 404 4
57 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/ns
e.html)"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.100.3 - - [06/Mar/2025:15:34:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
dinhthithanhtam-b22dcat253@dinhthithanhtamb22dcat253-virtual-machine:/var/log/ap
ache2$ cat access.log | grep "Nmap"Firefox"
```

```
Nguoi thuc hien: Dinh Thi Thanh Tam
MSV: B22DCAT253
Ngay thuc hien: 06/03/2025
```

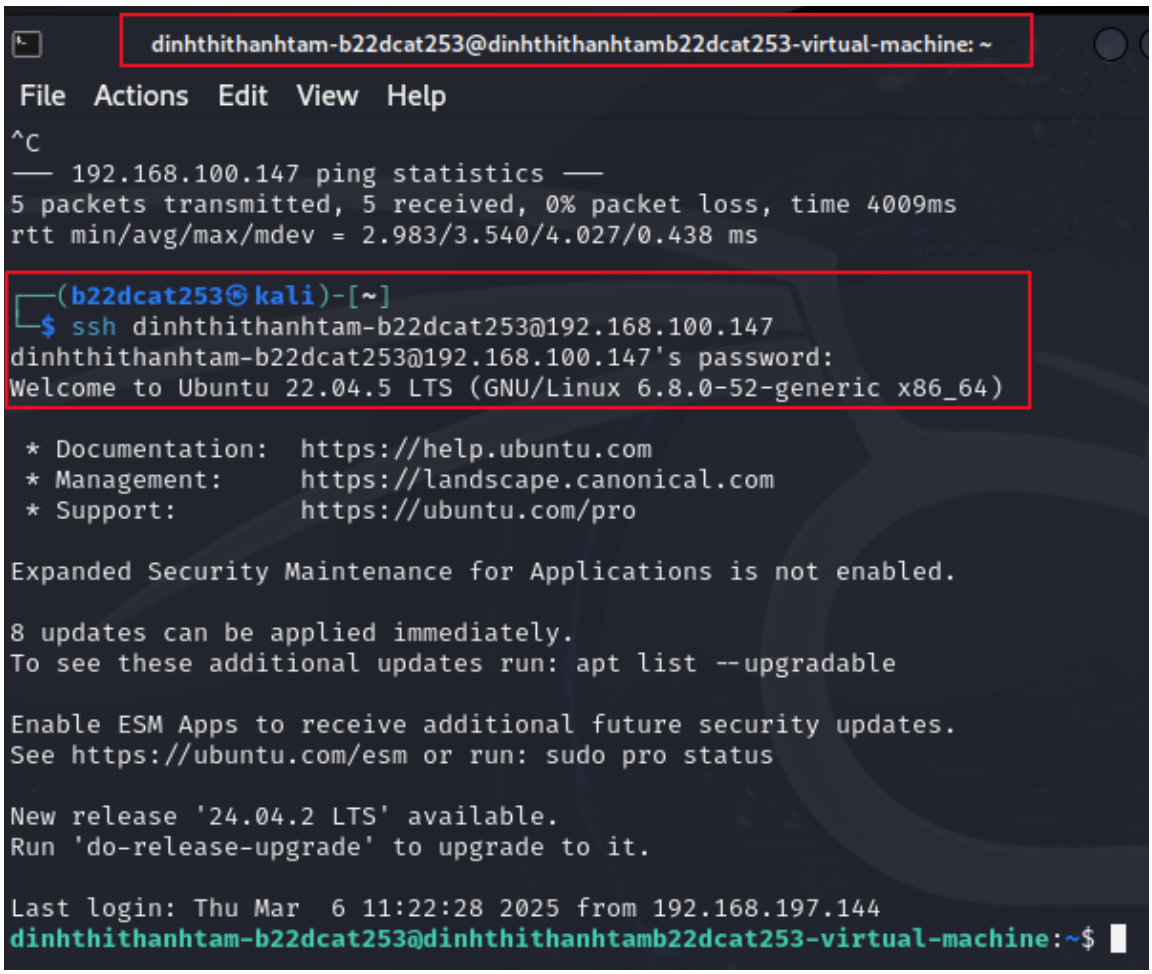
➔ Minh chứng: ảnh trên là minh chứng kết quả lọc dữ liệu dùng grep trên file log của máy nạn nhân, trong ảnh chụp có phần tên máy có chứa tên và mã sinh viên.

2.2.2 Phân tích log sử dụng gawk trong Linux

2.2.2.1 Tạo tài khoản mới trên máy Linux Internal Victim

- Trên máy Kali Attack, thực hiện kết nối SSH đến Linux Internal Victim:

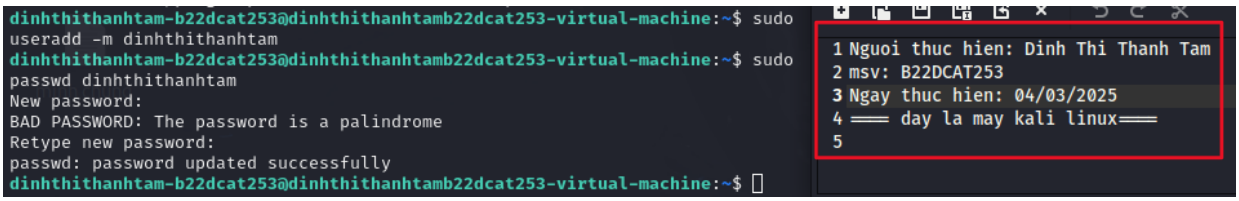
  ssh user@IP_VICTIM



- Sau khi đăng nhập thành công, tạo một tài khoản mới:

  sudo useradd -m <tên_sinh_viên>

  sudo passwd <tên_sinh_viên>



- Nhập mật khẩu tùy chọn hai lần để xác nhận.
- Thay đổi mật khẩu cho tài khoản mới

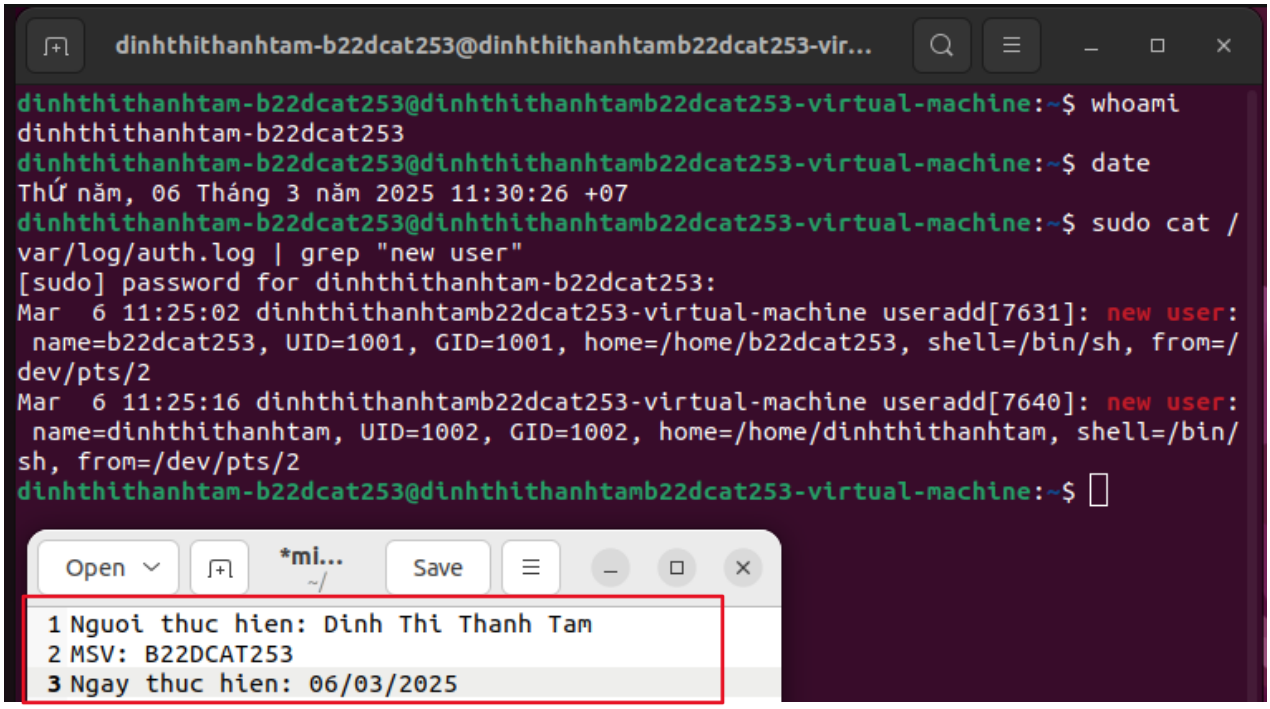
  sudo passwd <tên_sinh_viên>

- Nhập mật khẩu mới và xác nhận.

2.2.2.2 Kiểm tra file log trên máy Linux Internal Victim

- Các tệp log quan trọng liên quan đến tài khoản người dùng thường nằm trong /var/log/, sử dụng lệnh sau để xem:

  sudo cat /var/log/auth.log | grep "new user"



- Kết quả log hiển thị:
    - User b22dcat253 được tạo (UID=1001, GID=1001, home /home/b22dcat253, shell /bin/sh)
    - User dinhthithanhtam được tạo (UID=1002, GID=1002, home /home/dinhthithanhtam, shell /bin/sh)
    - Cả hai tài khoản được tạo từ /dev/pts/2, nghĩa là quá trình tạo tài khoản có thể được thực hiện từ một phiên terminal từ xa.
- Nhận xét và đánh giá
    - Việc tạo hai tài khoản mới xuất hiện trong file /var/log/auth.log, đây là bằng chứng hệ thống về việc thêm user.
    - Các tài khoản này có UID khác nhau, cho thấy chúng được tạo như người dùng mới thay vì ghi đè tài khoản cũ.
    - Log cho biết user mới được tạo từ /dev/pts/2, thường là một phiên SSH hoặc terminal từ xa.

2.2.2.3 Truy vấn log từ máy Kali Attack

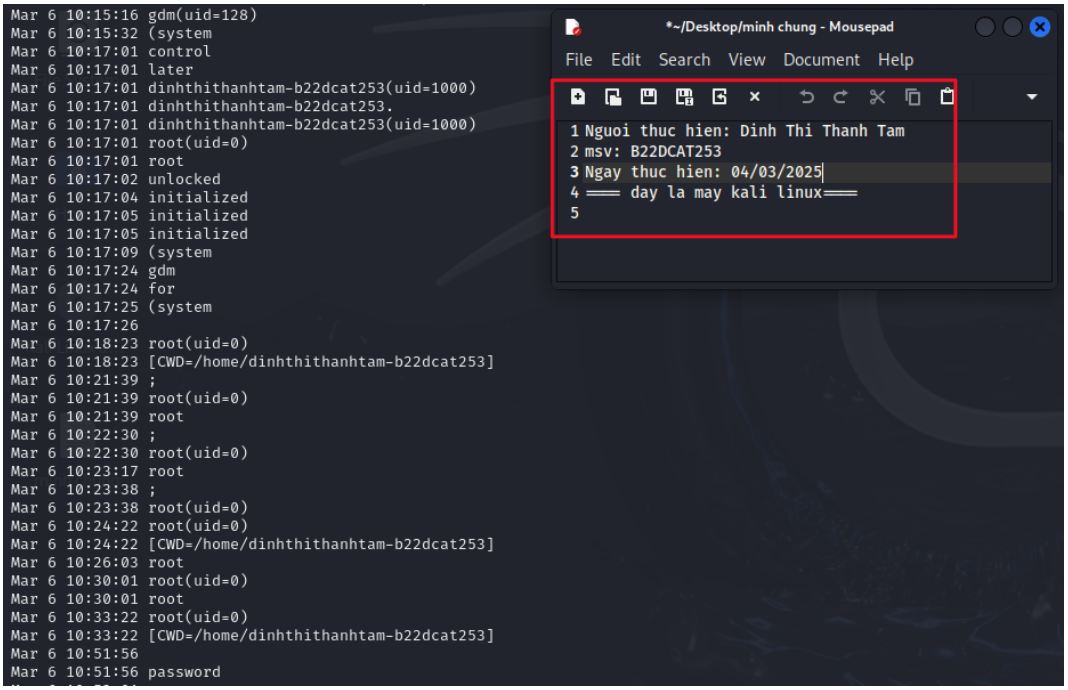
- Từ máy Kali, dùng SSH để truy vấn file log trên Linux Internal Victim:

  ssh user@IP_VICTIM "cat /var/log/auth.log | grep '<tên_sinh_viên>'"

- Dùng gawk để lọc và in dữ liệu mong muốn
- Sau khi tìm thấy thông tin bằng grep, ta sử dụng gawk để trích xuất và in nội dung mong muốn. Ví dụ:

ssh user@IP_VICTIM "cat /var/log/auth.log | grep 'new user' | gawk '{print \$1, \$2, \$3, \$11}'"

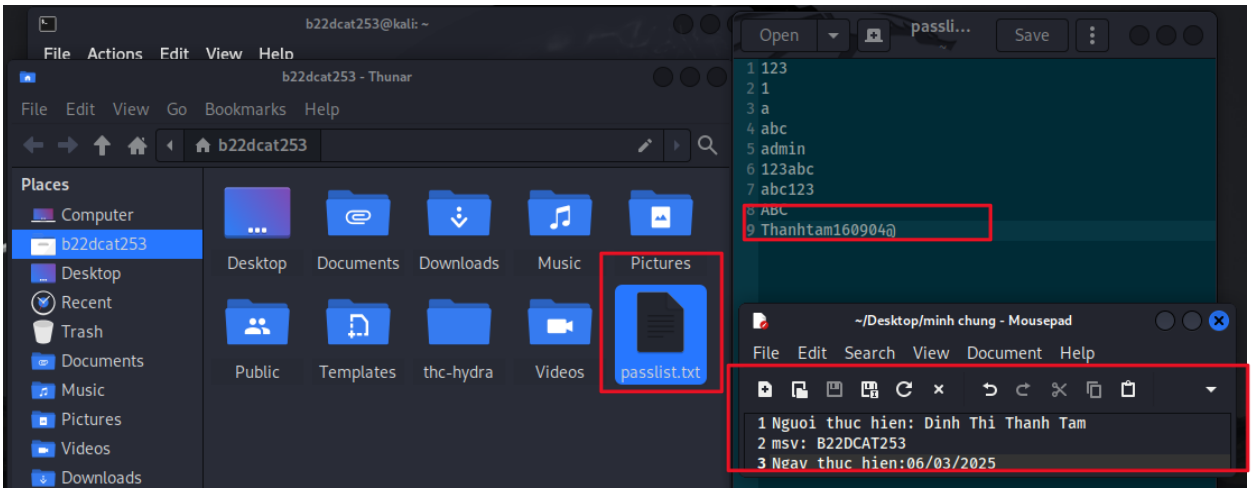
- Trong đó:
    - $1, $2, $3: Thời gian tạo user.
    - $11: Tên tài khoản được tạo.



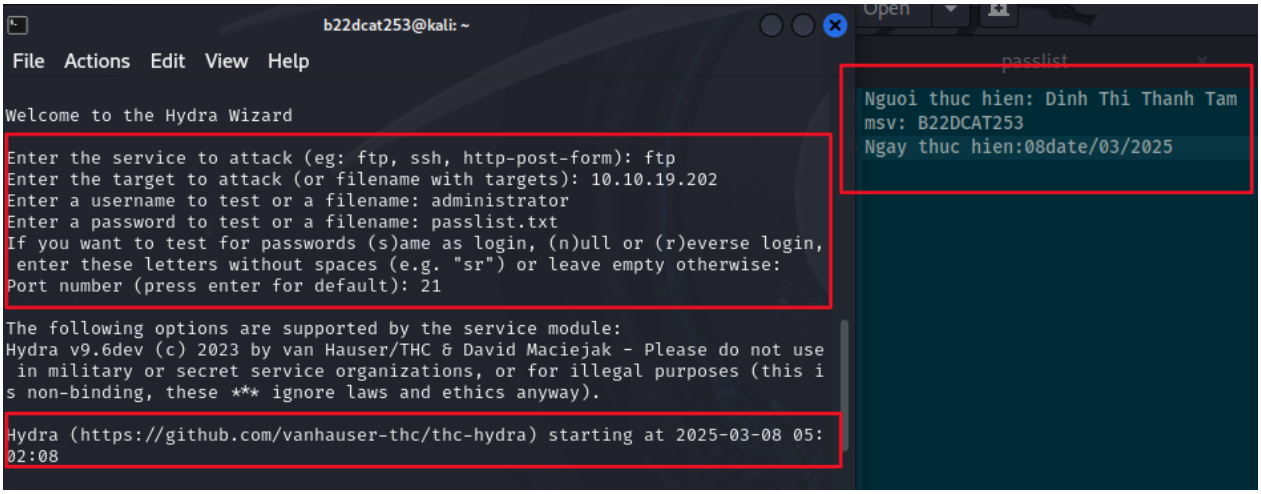
2.2.3 Phân tích log sử dụng find trong Windows

2.2.3.1 Sử dụng xHydra để brute-force FTP

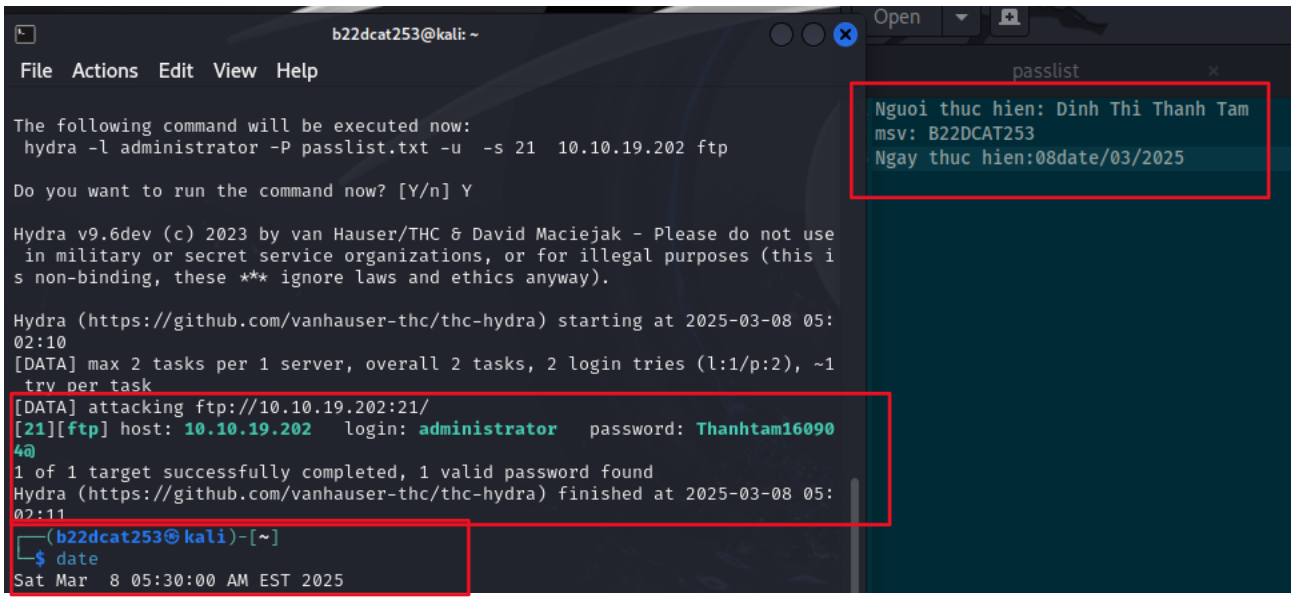
- Tạo file passlist.txt để lưu trữ các mật khẩu có thể được đặt để quét trên máy nạn nhân trng đó có 1 mật khẩu đúng để việc thử nghiệm quét được thành công



- Mở terminal trên Kali Linux và mở hydra:
- Nhập target: 10.10.19.202 (ip máy nạn nhân)
- Nhập username: administrator
- Nhập password là danh sách mật khẩu vừa tạo: passlist.txt



- Sau đó tiến hành quét mật khẩu trên máy nạn nhân:



➔ Thành công tìm được mật khẩu nghĩa là cuộc tấn công brute-force đã tìm thấy mật khẩu đúng.

2.2.3.2 Phân Tích Log FTP trên Windows Server 2019

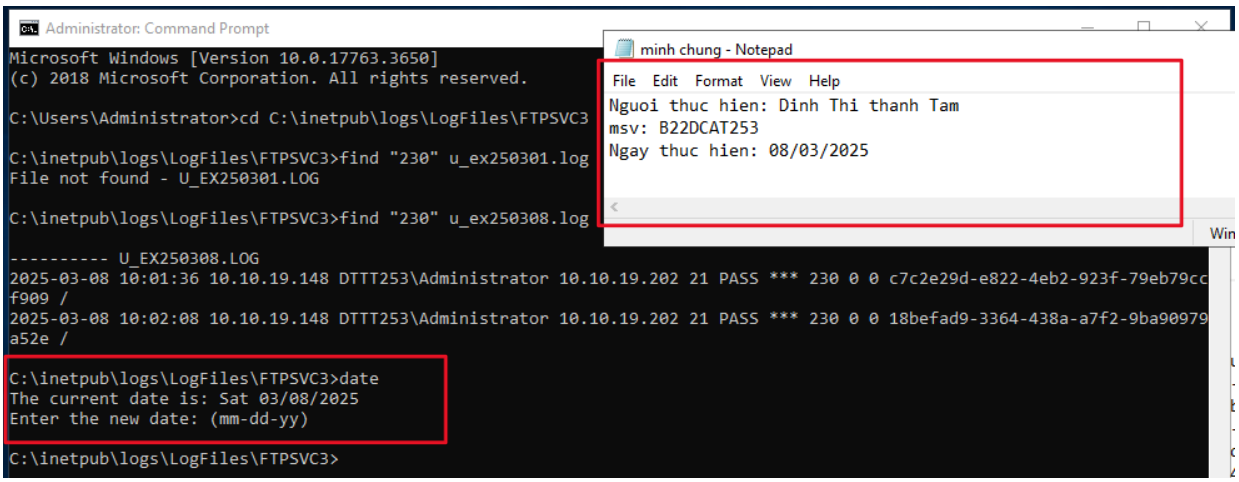
Thực hiện phân tích log FTP trên máy Windows Server 2019 External Victim sau khi thử nghiệm brute-force tấn công. Mục tiêu là tìm kết quả đăng nhập thành công từ file log FTP

- Điều hướng đến thư mục chứa log FTP
- Mở Command Promp (cmd.exe) trên Windows Server 2019
- Điều hướng đến thư mục chứa log của Microsoft FTP Server

  Cd C:\inetpub\log\LogFiles\FTPSVC3

- Chọn file log có ngày tháng phù hợp với thời điểm thực hiện tấn công. Ngày 08-03-2025
- Để lọc kết quả đăng nhập thành công, tìm mã 230 trong log:

  Find "230" u_ex250308.log



➔ Mã 230 trong log FTP có nghĩa là đăng nhập thành công.

KẾT LUẬN

Bài thực hành đã giúp phân tích log hệ thống để xác định dấu vết tấn công. Thông qua các công cụ như grep, gawk trên Linux và find trên Windows, giúp có thể lọc và tìm kiếm dữ liệu liên quan đến cuộc tấn công. Kết quả cho thấy log ghi lại các lần đăng nhập thành công sau tấn công brute-force bằng Hydra. Dữ liệu log này được lưu lại để phục vụ phân tích bảo mật.

TÀI LIỆU THAM KHẢO

[1] grep: https://linuxcommand.org/lc3_man_pages/grep1.html

[2] gawk: http://www.gnu.org/software/gawk/manual/gawk.html

[3] find:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find

[4] xhydra: http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html